UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,983	03/31/2004	Hashem Mohammad Ebrahimi	1565.069US1	9751

21186 7590 02/01/2008
SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
GYORFI, THOMAS A	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
02/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/814,983	**Applicant(s)** EBRAHIMI ET AL.	
	Examiner Tom Gyorfi	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)	4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) □ Notice of Informal Patent Application
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/21/07*.	6) □ Other: _____.

DETAILED ACTION

1. Claims 1-26 remain for examination. The correspondence filed 11/21/07 amended claims 1, 8, 13-15, and 21.

Response to Arguments

2. Applicant's arguments with respect to claims 1-26 have been considered but are moot in view of the new ground(s) of rejection.

3. The rejections of claims 13 and 14 under 35 USC 112 have been withdrawn, in view of Applicant's amendment of those claims.

4. Applicant's has traversed the Examiner's multiple invocations of Official Notice by requesting that Examiner provide some concrete evidence supporting the assertions made therein; however, this fails to take into account that Examiner fulfilled that obligation under MPEP 2144 by citing the "RFC2246" reference in the Office Action to illustrate those limitations that represented common knowledge in the art (see the Office Action of 8/22/07: the rejection of claims 13 & 17 on page 8 cites page 41 of RFC2246 for support, while the rejection of claim 24 on page 9 cites page 23 of RFC2246 for support). Applicant had ample opportunity to consider the additional reference in crafting a response to the rejections, but has apparently failed to do so. Accordingly, Applicant's traversal of the Official Notice(s) is inadequate and thus, by rule, is now taken as an admission of prior art as permitted by MPEP 2144.03(c).

Information Disclosure Statement

5. The information disclosure statement (IDS) submitted on 11/21/07 has been considered by the Examiner.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-26 are rejected under 35 U.S.C. 102(b) based upon a public use or sale of the invention. The Netscape Proxy Server Version 3.5 for Unix (hereinafter, "Netscape") implemented all the limitations of the claims, as evidenced by the Netscape Proxy Server Version 3.5 for Unix Administrator's Guide (all chapters published no later than 2/25/98, and originally supplied by the Applicant in the IDS of 3/31/04).

Regarding claim 1:

Netscape discloses a method comprising: receiving a secure communication request from a client (Chapter 14, page 2, Figure 14.1 and 1st paragraph); identifying a domain identification associated with the request (inherent to proxying in general; cf. Chapter 6, e.g. "Enabling Proxying for a Resource"); and routing the request to a proxy based on the domain identification, wherein the proxy communicates securely with the external domain via a first set of unique session keys used for the local domain accelerator and the external domain (Chapter 14, "Setting up Client Authentication in a Reverse Proxy", cf. "Content Server Authenticates Proxy") and separately the local domain accelerator communicates securely with the client via a second set of unique session keys used for the local domain accelerator and the client to communicate (Chapter 14, "Setting up Client Authentication in a Reverse Proxy", cf. "Proxy Authenticates Client") and the first set of session keys and the second set of session keys are different from one another (Ibid, by virtue of being inherent to the multiple SSL connections disclosed) and wherein the client believes communication that the client has with the local domain accelerator is occurring with the external domain but in fact it occurs with the local domain accelerator via the second set of session keys ("What Netscape Proxy Server Provides", 2nd and 5th paragraphs; Chapter 7, "How Reverse Proxying Works"), and wherein the local domain accelerator caches data from the external domain for servicing the request of the client (see all of Chapter 9, beginning with "How Caching Works").

Regarding claim 8:

Netscape discloses a method comprising: receiving a secure request forwarded from a proxy, the secure request originating from a client and destined for an external domain (Chapter 14, page 2, Figure 14.1 and 1st paragraph); establishing a secure communication with the client by providing the client a certificate associated with an external domain (Chapter 5, "Controlling Access with Client Certificates") and wherein the secure communication entails using a first set of session keys to communicate securely with the client and the client believes after receiving the certificate that communication is occurring with the external domain (Chapter 14, “Setting up Client Authentication in a Reverse Proxy”, cf. “Proxy Authenticates Client”; Chapter 7, “How Reverse Proxying Works”); and servicing the client with data that is acquired from the external domain, and wherein a portion of that data is used to service the request (all of Chapter 9), and wherein separate communication is securely established with the external domain using a second set of session keys different from the first set of session keys (Chapter 14, “Setting up Client Authentication in a Reverse Proxy”, cf. “Content Server Authenticates Proxy”).

Regarding claim 15:

Netscape discloses a system comprising: a proxy (e.g. “What Netscape Proxy Server Provides”); and a local domain accelerator (Ibid, but particularly the 3rd and 4th paragraphs; cf. Chapter 9, “How Caching Works”) wherein a client securely requests an external domain and the proxy routes the request to the local domain accelerator [i.e. itself], the local domain accelerator securely communicates with the external domain and services the client via secure communications between the local domain accelerator and the client (Chapter 14, e.g. "Tunneling SSL through the Proxy Server"), and wherein the proxy communicates securely with the external domain via a first set of unique session keys used for the local domain accelerator and the external domain (Chapter 14, “Setting up Client Authentication in a Reverse Proxy”, cf. “Content Server Authenticates Proxy”) and separately the local domain accelerator communicates securely with the client via a second set of unique session keys used for the local domain accelerator and the client to communicate (Chapter 14, “Setting up Client Authentication in a Reverse Proxy”, cf. “Proxy Authenticates Client”) and the first set of session keys and the second set of session keys are different from one another (Ibid, by virtue of being inherent to the multiple SSL connections disclosed) and wherein the client believes communication that the client has with the local domain accelerator is occurring with the external domain but in fact it occurs with the local domain accelerator via the second set of session keys ("What Netscape Proxy Server Provides", 2nd and 5th paragraphs; Chapter 7, “How Reverse Proxying Works”).

Regarding claim 21:

Netscape discloses a system comprising: a local domain accelerator (“What Netscape Proxy Server Provides”, 3rd and 4th paragraphs; Chapter 9, "How Caching Works"); and wherein the local domain accelerator securely communicates with a client as if the local domain accelerator was an external domain [i.e. a proxy] and securely communicates with the external domain for purposes of acquiring data from the external domain (Chapter 14, e.g. "Tunneling SSL through the Proxy Server"), wherein the proxy communicates securely with the external domain via a first set of unique session keys used for the local domain accelerator and the external domain (Chapter 14, “Setting up Client Authentication in a Reverse Proxy”, cf. “Content Server Authenticates Proxy”) and separately the local domain accelerator communicates securely with the client via a second set of unique session keys used for the local domain accelerator and the client to communicate (Chapter 14, “Setting up Client Authentication in a Reverse Proxy”, cf. “Proxy Authenticates Client”) and the first set of session keys and the second set of session keys are different from one another (Ibid, by virtue of being inherent to the multiple SSL connections disclosed) and wherein the client believes communication that the client has with the local domain accelerator is occurring with the external domain but in fact it occurs with the local domain accelerator via the second set of session keys ("What Netscape Proxy Server Provides", 2nd and 5th paragraphs; Chapter 7, “How Reverse Proxying Works”).

Regarding claims 2 and 19:

Netscape further discloses one of a forward proxy and a transparent proxy ("What Netscape Proxy Server Provides", 2nd and 5th paragraphs; Chapter 14, "Using Encryption in the Proxy Server, 2nd paragraph).

Regarding claims 3, 16, and 23:

Netscape further discloses returning, by the local domain accelerator, to the client a domain certificate that identifies the local domain accelerator as the external domain to the client (Chapter 14, pages 3-4, “Enabling SSL on Your Server”).

Regarding claims 4 and 18:

Netscape further discloses establishing a Secure Sockets Layer (SSL) handshake between the client and the local domain accelerator to service the request, wherein the client believes that the handshake is with external domain (Chapter 14).

Regarding claim 5:

Netscape further discloses intercepting the request that originates from the client to the external domain (inherent to proxies by definition; see also Chapter 6, "Sending the Client's IP Address to the Server", wherein by default the proxy intercepts a client request to replace the client's IP address with the proxy's IP address).

Regarding claims 6 and 10:

Netscape further discloses accessing, by the local domain accelerator, caching services for caching and managing the data (all of Chapter 9).

Regarding claim 7:

Netscape further discloses wherein stripping a host header from the request, host header being the domain identifier that identifies the external domain (inherent to proxies by definition; see also Chapter 5, "Allowing Access to a Resource").

Regarding claim 9:

Netscape further discloses acting as the external domain when interacting with the client (inherent to being a transparent proxy: "What Netscape Proxy Server Provides", 2nd and 5th paragraphs; Chapter 14, "Using Encryption in the Proxy Server, 2nd paragraph).

Regarding claim 11:

Netscape further discloses acquiring at least a portion of the data from the external domain in advance of a subsequent request for that portion of the data, wherein the subsequent request is issued from the client (Chapter 9, "Using Cache Batch Updates").

Regarding claim 12:

Netscape further discloses interacting securely with the external domain to acquire the data housed in the local cache (Ibid; secure connections disclosed in Chapter 14, e.g. "Setting Up Client Authentication in a Reverse Proxy").

Regarding claims 13 and 17:

Netscape further discloses wherein interacting securely further includes mutually signing interactions transmitted between the local domain accelerator and the external domain, as this is inherent to SSL ("The Secure Socket Layer Protocol (SSL)", page 3, "SSL – Authentication and Integrity"; cf. Netscape, Chapter 5, "Controlling Access with Client Certificates"; see also RFC2246, e.g. page 41).

Regarding claim 14:

Netscape further discloses using the proxy to establish a secure communications channel between the local domain accelerator and the external domain (Chapter 14, e.g. Figure 14.2 and "Setting Encryption Preferences").

Regarding claims 20 and 22:

Netscape further discloses wherein the proxy creates a secure communications tunnel between the client and the local domain accelerator and the proxy creates a secure communications channel between the local domain accelerator and the external domain (Chapter 7, “Setting Up a Secure Reverse Proxy”; Chapter 14, “Setting up Client Authentication in a Reverse Proxy”).

Regarding claim 24:

SSL as implemented by Netscape inherently requires an exchange of certificates during communications between two parties (see “The Secure Sockets Layer Protocol (SSL)”, page 3, “SSL – Authentication and Integrity”; cf. Netscape, Chapter 5, “Controlling Access with Client Certificates”; see also RFC2246, page 23).

Regarding claim 25:

Netscape further discloses wherein the client is a browser using SSL (e.g. Netscape Navigator: “What Netscape Proxy Server Provides”, 6th paragraph; Chapter 14, “What is HTTPS?”), and the local domain accelerator intercepts and forwards communications toward a proxy and the proxy forwards communications to the local domain accelerator where the local domain accelerator presents itself securely to the client as if it were the external domain (Chapter 6, “Mapping URLs to Other URLs”; Chapter 7, “How Reverse Proxying Works” and “Setting Up a Secure Reverse Proxy”).

Regarding claim 26:

Netscape further discloses a plurality of external sites featuring a plurality of services (e.g. Chapter 7, "Proxying for Load Balancing").

Claim Rejections - 35 USC § 103

8. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

9. Claims 1-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Birrell et al. (U.S. Patent 5,805,803) in view of the Netscape Proxy Server v3.5.

Regarding claim 1:

Birrell discloses a method comprising: receiving a secure communication request from a client (col. 4, lines 5-20); identifying a domain identification associated with the request (Ibid); and routing the request to a proxy based on the domain identification, wherein the proxy communicates securely with the external domain and securely with the client (col. 4, lines 15-30).

Although Birrell discloses wherein the client and the local domain accelerator use a first set of session keys to communicate with each other (via an SSL connection: see col. 3, lines 5-10 and col. 4, lines 13-25), Birrell does not disclose wherein the local domain accelerator and the external domain use a second set of session keys different from the first set to communicate with each other, in such a manner that the client believes that it is communicating directly with the external domain; nor does Birrell

discloses that the proxy/local domain accelerator caches data from the external domain. However, as discussed above, all limitations not disclosed by Birrell are disclosed by Netscape as being techniques well within the abilities of one of ordinary skill in the art to incorporate into a proxy system (see the rejection of claim 1 under 35 USC 102(b) above). Thus, the claim is obvious because all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time the invention was made.

Regarding claim 8:

Birrell discloses a method comprising: receiving a secure request forwarded from a proxy, the secure request originating from a client and destined for an external domain (col. 4, lines 5-15; cf. col. 3, lines 5-15); establishing a secure communication with the client by providing the client a certificate associated with an external domain (col. 4, lines 35-45); and servicing the client with data that is acquired from the external domain, and wherein a portion of that data is used to service the request (col. 4, lines 45-50).

Although Birrell discloses wherein the client and the local domain accelerator use a first set of session keys to communicate with each other (via an SSL connection: see col. 3, lines 5-10 and col. 4, lines 13-25), Birrell does not disclose wherein the local domain accelerator and the external domain use a second set of session keys different from the first set to communicate with each other, in such a manner that the client believes that it is communicating directly with the external domain; nor does Birrell

discloses that the proxy/local domain accelerator caches data from the external domain. However, as discussed above, all limitations not disclosed by Birrell are disclosed by Netscape as being techniques well within the abilities of one of ordinary skill in the art to incorporate into a proxy system (see the rejection of claim 8 under 35 USC 102(b) above). Thus, the claim is obvious because all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time the invention was made.

Regarding claim 15:

Birrell discloses a system comprising: a proxy (element 143 of Figure 1); and a local domain accelerator (col. 2, lines 29-31) wherein a client securely requests an external domain and the proxy routes the request to the local domain accelerator [i.e. itself], the local domain accelerator securely communicates with the external domain and services the client via secure communications between the local domain accelerator and the client (col. 2, lines 20-60).

Although Birrell discloses wherein the client and the local domain accelerator use a first set of session keys to communicate with each other (via an SSL connection: see col. 3, lines 5-10 and col. 4, lines 13-25), Birrell does not disclose wherein the local domain accelerator and the external domain use a second set of session keys different from the first set to communicate with each other, in such a manner that the client believes that it is communicating directly with the external domain; nor does Birrell

discloses that the proxy/local domain accelerator caches data from the external domain. However, as discussed above, all limitations not disclosed by Birrell are disclosed by Netscape as being techniques well within the abilities of one of ordinary skill in the art to incorporate into a proxy system (see the rejection of claim 15 under 35 USC 102(b) above). Thus, the claim is obvious because all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time the invention was made.

Regarding claim 21:

Birrell discloses a system comprising: a local domain accelerator (element 140 of Figure 1; cf. col. 2, lines 29-31); and wherein the local domain accelerator securely communicates with a client as if the local domain accelerator was an external domain [i.e. a proxy] and securely communicates with the external domain for purposes of acquiring data from the external domain (col. 2, lines 20-60).

Although Birrell discloses wherein the client and the local domain accelerator use a first set of session keys to communicate with each other (via an SSL connection: see col. 3, lines 5-10 and col. 4, lines 13-25), Birrell does not disclose wherein the local domain accelerator and the external domain use a second set of session keys different from the first set to communicate with each other, in such a manner that the client believes that it is communicating directly with the external domain; nor does Birrell discloses that the proxy/local domain accelerator caches data from the external domain.

However, as discussed above, all limitations not disclosed by Birrell are disclosed by Netscape as being techniques well within the abilities of one of ordinary skill in the art to incorporate into a proxy system (see the rejection of claim 21 under 35 USC 102(b) above). Thus, the claim is obvious because all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed with no change in their respective functions, and the combination would have yielded predictable results to one of ordinary skill in the art at the time the invention was made.

Regarding claims 2 and 19:

Birrell further discloses one of a forward proxy and a transparent proxy (col. 2, lines 45-50).

Regarding claims 3, 16, and 23:

Birrell further discloses returning, by the local domain accelerator, to the client a domain certificate that identifies the local domain accelerator as the external domain to the client (col. 4, lines 35-40).

Regarding claims 4 and 18:

Birrell further discloses establishing a Secure Sockets Layer (SSL) handshake between the client and the local domain accelerator to service the request, wherein the client believes that the handshake is with external domain (col. 3, lines 5-15 & 55-60).

Regarding claim 5:

Birrell further discloses intercepting the request that originates from the client to the external domain (col. 4, lines 13-17).

Regarding claims 6 and 10:

Netscape further discloses accessing, by the local domain accelerator, caching services for caching and managing the data (all of Chapter 9).

Regarding claim 7:

Birrell further discloses wherein stripping a host header from the request, host header being the domain identifier that identifies the external domain (col. 5, lines 1-10).

Regarding claim 9:

Birrell further discloses acting as the external domain when interacting with the client (i.e. a conventional proxy server, as per col. 4, lines 45-50).

Regarding claim 11:

Netscape further discloses acquiring at least a portion of the data from the external domain in advance of a subsequent request for that portion of the data, wherein the subsequent request is issued from the client (Chapter 9, "Using Cache Batch Updates").

Regarding claim 12:

Birrell further discloses interacting securely with the external domain to acquire the data housed in the local cache (col. 4, lines 50-60).

Regarding claims 13 and 17:

Birrell further discloses wherein interacting securely further includes mutually signing interactions transmitted between the local domain accelerator and the external domain (col. 4, lines 30-60; it is also admitted prior art that mutually signing interactions is intrinsically part of the SSL protocol – see RFC2246, e.g. page 41).

Regarding claim 14:

Birrell further discloses using the proxy to establish a secure communications channel between the local domain accelerator and the external domain (col. 4, 50-60).

Regarding claims 20 and 22:

Birrell further discloses wherein the proxy creates a secure communications tunnel between the client and the local domain accelerator and the proxy creates a secure communications channel between the local domain accelerator and the external domain (col. 4, lines 45-65).

Regarding claim 24:

It is now taken as admitted prior art that SSL by definition requires an exchange of certificates during communications between two parties (see RFC2246, e.g. page 23, “peer certificates”). Additionally, Netscape discloses this limitation (Chapter 5, “Controlling Access with Client Certificates").

Regarding claim 25:

Birrell further discloses wherein the client is a browser (col. 3, lines 20-25), uses SSL (col. 3, lines 5-10), and the local domain accelerator intercepts and forwards communications toward a proxy and the proxy forwards communications to the local domain accelerator where the local domain accelerator presents itself securely to the client as if it were the external domain (col. 4, lines 30-60).

Regarding claim 26:

Birrell further discloses a plurality of external sites featuring a plurality of services (col. 3, lines 15-20).

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- “The Secure Sockets Layer Protocol (SSL)” by Taher Elgamal establishes several of the claimed limitations as being inherent to SSL

- “Modifications to the SSL protocol for TLS” establishes that TLS as defined in RFC2246 is for all intents and purposes identical to SSL, differing only in those aspects that are not germane to the claimed invention
- “[SSL-Talk List FAQ] Secure Sockets Layer Discussion List FAQ v1.1.1” confirms that SSL and TLS are essentially identical (page 3, as indicated) and that Netscape Proxy Server v3.5 is operable to create multiple SSL connections, one between the client and the proxy and a second between the proxy and the server (page 7, as indicated)
- “Tunneling TCP based protocols through Web proxy servers" by Ari Luotonen also describes tunneling SSL through a proxy

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
1/24/08